Towards CCTV-aware Routing and Navigation for Privacy, Anonymity, and Safety – Feasibility Study in Jyväskylä

Tuomo Lahtinen[§], Lauri Sintonen[§], Hannu Turtiainen[¶], Andrei Costin[¶] ⊛
University of Jyväskylä
Jyväskylä, Finland
[¶]{turthzu,ancostin}@jyu.fi,
[§]{tuomo.t.lahtinen,lauri.m.j.sintonen}@student.jyu.fi
⊛ Corresponding and original idea's author.

***Abstract*—In order to withstand the ever-increasing invasion of privacy by CCTV cameras and technologies, on par *CCTV-aware solutions* must exist that provide privacy, safety, and cybersecurity features. We argue that a first important step towards such CCTV-aware solutions must be a mapping system (e.g., Google Maps, OpenStreetMap) that provides both privacy and safety routing and navigation options. Unfortunately, to the best of our knowledge, there are no mapping nor navigation systems that support CCTV-privacy and CCTV-safety routing options.**

At the same time, in order to move the privacy vs. safety debate related to CCTV surveillance cameras from purely subjective to data-driven and evidence-based domain, it would require to implement and evaluate a globally-relevant CCTV-aware routing and navigation system. This however, would require a tremendous initial effort without any guarantees about the feasibility and the end result. Therefore, we propose first a p reliminary evaluation of such CCTV-aware technology at a small scale, for example a medium-sized European city.

In this paper, we explore the feasibility of a CCTV-aware routing and navigation solution. The aim of this feasibility exploration is to understand what are the main impacts of CCTV on privacy, and what are the challenges and benefits to building such technology. We evaluate our approach on six (6) pedestrian walking routes within the downtown area of the city of Jyväskylä, Finland. We first map a total of 450 CCTV cameras, and then experiment with routing and navigation under several different configurations to *coarsely model* the possible cameras' parameters and coverage from the real-world.

We report two main results. First, our preliminary findings support the overall feasibility of our approach. Second, the results also reveal a data-driven worrying reality for persons wishing to preserve their privacy/anonymity as their main living choice. When modelling cameras at their low performance end, a privacy-preserving route has on average a 1.5x distance increase when compared to generic routing. When modelling cameras at their medium-to-high performance end, a privacy-preserving route has on average a 5.0x distance increase, while in some cases there are no routes possible at all, i.e., privacy/anonymity must be given up to reach the destination. These results further support and encourage both global mapping of CCTV cameras and refinements to camera modelling and underlying technology in the context of more accurate CCTV-aware routing and navigation.

I. Introduction

CCTV camera surveillance has been spread all over the world and major cities have a very dense network of surveillance cameras. People can not move in streets or cities without getting caught by surveillance. Currently, it is estimated there are about 770 millions CCTV cameras around the globe, and their number is casually predicted to surpass 1 billion in 2021 [9]. For example, a study in UK finds that on average a person enters a CCTV camera view 300 times a day [3]. A similar study in the US puts that number at 50+ times a day, despite the more worrying fact that the average US respondent *assumed it was 4 cameras or less* [19]. This patronizing way of measuring people's every movement is frightening when it is combined with face recognition. Hu et al. [18] surveyed and described visual surveillance and great progress in face recognition. Since then face recognition has been developed a lot and very accurate surveillance is possible with modern cameras.

In order to withstand this ever-increasing invasion of privacy by CCTV cameras and technologies, on par *CCTV-aware solutions* must exist that provide privacy, safety, and cybersecurity features. We argue that a first important step towards such CCTV-aware solutions must be a mapping system (e.g., Google Maps, OpenStreetMap) that provides both privacy and safety routing and navigation options.

At present, there is a myriad of route planning algorithms, software, and services [6], [11], [26], [33], [34], [38]. Therefore a wide variety of solutions are available: open- and closed-source, online and offline, free and paid. However, to the best of our knowledge, none of the currently available algorithms, software, and services provide *CCTV-aware* route planning and navigation. In our approach, we propose two routing options, namely *privacy-first* and *safety-first*. Privacy-first routing calculates and optimizes the route in order to avoid the field of view of cameras along the generated route between departure and arrival points. Such a scenario is desirable anytime (e.g., day-time, night-time) when privacy/anonymity is important, or there are no GDPR-enforceable guarantees on the CCTV footage. Safety-first routing is somewhat opposite to the goals of privacy-first routing. It calculates and optimizes the route in order to guarantee the user that the route follows the streets with as many cameras as possible. We call it safety-

ISSN 2305-7254

first because the intention is to increase the chances of physical safety for the user. Such a scenario is desirable for example when visiting known unsafe or unknown areas, or when navigating at night. Generally speaking, in a model where all the CCTV cameras are mapped, the *safety-first* would be very close to normal routing because we expect the cameras to be everywhere. However, there may still be cases where *safety-first* routes would be different from normal routes because route optimization does not take time nor distance into account but rather maximizing the exposure to the CCTV cameras. However it is important to note that at present none of these two routing modes can provide 100% guarantee. One reason is the lack of accurate and up-to-date data about CCTV camera properties (e.g., model, position, owner). Another reason is that our model is not yet fully refined and does not support sub-meter routing accuracy.

To the best of our knowledge, we are the first to propose and work on such features at present and we are unaware of any project or service developing or offering such route planning options. We build our current work atop and in relation to another contribution of ours, where we developed and demonstrated the first and only Computer Vision (CV) models to scalably and accurately detect CCTV camera object in images (e.g., street-level, indoors) and we achieve an accuracy of up to 98.7% [40]. Our bigger vision is that using those CV models we can instantly, accurately and globally map the vast majority of CCTV cameras visible on street-level imagery services such as Google Street View [2], Yandex Street Panoramas, Baidu Total View, Mapillary. In our vision, once this localization and mapping is completed, we can experiment further at large scale with the CCTV-aware routing and navigation technology introduced in current paper.

A. Contributions

- We are the first to introduce and model CCTV-aware *privacy-first* and *safety-first* routing scenarios as relevant for modern digitized lifestyle.
- We model, quantify and report CCTV cameras' impact on privacy for pedestrian routes using a modern city downtown area as experimental ground.
- We outline the challenges and the benefits of pursuing these experiments and models at global scale.
- We present Jyväskylä as the first city to experiment and benefit from CCTV-aware technology.

II. Related Work

OpenStreetMap (OSM) is a collaborative project to create a free editable map of the world, with millions of users and large number of contributors. There are hundreds of OSM-based services and routers [6], [26], [33], [34], [38], [44]. Many of the routers are related to basic driving, walking or cycling navigation, and others focus on more specific use-cases ranging from highlighting curvy roads [14] to more specialized navigation for cyclists [7], [8], [22], wheelchair routing [16], [20], [48], and routing according to sun or shade [10], [29], [32]. None of the known solutions provide *CCTV-aware* route planning and navigation, in particular focusing on privacy-first routing.

Olaverri Monreal et al. [32] proposed a router that follows shaded paths. In 2018, Ma [29] introduced *Parasol*, which is a routing solution that *"uses high-resolution elevation data to simulate sunshine and constructs routes that keep users in the sun or shade"*. The author released the code as open-source [28]. Following the work of Ma [29], more recently Deilami et al. [10] introduced *Shadeways*, a route planning software to keep its users in shade. Their solution uses heat information and tree shading data in the process of determining the route. While approaches such as *Parasol* [29] and *Shadeways* [10] are inspiring and in theory could be adapted for CCTV-aware routing, they are not directly usable because of the differences in the underlying data requirements. In addition, neither *Parasol* nor *Shadeways* try to solve some core challenges with OSM data. For example, in OSM a way object [47] is represented as a line with no actual width on the map [24], whereas in reality a way is not a line but a space.

Some other authors use a safety-first approach when pursuing routing solutions. Bao et al. [5] present a method for pedestrians to find safer routes by investigating *"the influences of landmark scarcity, visibility, lighting condition, road width and turning tolerance on perceived safety and comprehensiveness"*. Hirozaku et al. [30] also observe the illumination in order to provide a safer route for pedestrians. Keler and Mazimpaka [21] aim towards routing in relatively dangerous areas within a city by utilizing Volunteered Geographic Information (VGI), i.e., crowdsourcing. Tessio et al. [31] provide a system which enables users to define customized pedestrian routes with green areas, social places and quieter streets.

Luxen and Vetter [25], [27] provide *Open Source Routing Machine (OSRM)*, an even more general routing backend which enables users to write their own routing profiles in Lua code [36] as well as to use *traffic updates* to set weights between any two connected and routable nodes [35]. Using *OSRM* profiles one can use any OSM tags to weigh the routing process. In our work we use *OSRM* and its routing profiles and *traffic updates* as our routing solution.

In order to successfully manage and update the OSM data, relevant OSM data editors are required. Indeed, many editors exist that can be used to edit OSM data. The most common of those with a graphical user interface are *iD*, *JOSM*, *Potlach 2*, *Vespucci* (Android) and *Go Map!!* (iOS) [42]. There are also more programmatic ways for editing OSM data. Two popular frameworks are *Osmosis* (Java) [46] and *Osmium* (C++) [39]. *Osmium* has also a Python wrapper, *PyOsmium* [17] which is used in our work. *GeoPandas* [12] and *Shapely* [15] are popular Python libraries for geometric manipulation of data, the latter of which is used in our work.

III. Experimental setup

In this section we present our experimental setup. We explore *pedestrian routing* scenarios where the main constraint on the computations is about the ability of modelled cameras to *recognize faces* or not. For *privacy-first* option, the optimization is about routing the user in such a way that cameras are far away enough hence making the *face recognition* task to be unsuccessful. For *safety-first* option, the optimization is about routing the user in such a way that user is at anytime close enough to at least one camera which can perform *face recognition* task successfully. The routing experiments are run on data collected from and relevant to the city of Jyväskylä,

Finland. In the future, we plan to extend the experiments to a more global scale.

A. Short introduction to routing engine

We base our experimental routing setup on *Open Source Routing Machine (OSRM)* [27] and its routing profiles [36] as well as its *traffic updates* [35]. However, the main contribution from a routing perspective relies on how we process OSM XML data, which is essentially an XML file containing a list of certain OSM elements: nodes, ways, and relations [45]. Data manipulation is needed to mitigate the fact that an OSM way object is primarily a line without width [47]. In order to reach sub-meter routing accuracy required for *CCTV-aware* (e.g., 1 meter can mean a difference between face recognition and face detection ability for the camera), the *OSM ways* need to have relevant width information associated. This information is required so that it is possible to allow routing through a way if only the other side of it is under the scope of a CCTV camera.

To mitigate the limitation of *OSM way* objects having no width [47], Lucas-Smith proposes representing streets more realistically as boxes or areas instead of lines [24]. This has inspired the approach used in our work. Instead of handling all the ways in an OSM file, we modify OSM data locally by splitting a way into two whenever there is a CCTV camera nearby. Then, if the scope of the CCTV camera covers only some of the way splits, it is still possible to traverse the others while maintaining privacy. In a screenshot of a view in *JOSM* [37], [43] (see Fig. 1), the teal-colored nodes (cyan squares) represent the camera and the points where one would enter under the scope of the camera. As the scope does not cover the whole way, namely all of the way splits, traversing the way still preserves privacy. It may however required that for the example in Fig. 1, the user is explicitly instructed to walk at the opposite edge of the street when arriving close to the area of CCTV camera coverage. Such granularity is challenging in many ways, including GPS accuracy, and even though it is not implemented in our routing system at this moment we plan it in our future roadmap.

B. Mapping of CCTV cameras

Before starting our experiments on different CCTV camera coverage models and corresponding route calculations, we have mapped a large number of CCTV cameras around Jyväskylä, which is a city in Central Finland with an urban area of about 100 square kilometers and a population of about 138.000. We mainly focused on its downtown and busiest areas.

We have managed to map around 450 cameras in the city of Jyv¨askyl¨a, as partly depicted in Fig. 2. For now, their localization and mapping was mostly performed manually (about 400 cameras) by moving around the city to discover CCTV/surveillance cameras. The rest (about 50 cameras) were localized and mapped using a novel and unique *in-browser plugin for annotation and crowdsourcing* tool (Fig. 3) that we have specifically developed for this project and its future needs. Thus, our browser annotation tool allows us to use large-scale crowdsourcing for computer vision training purposes. It also enables us to annotate and to precisely localize CCTV cameras

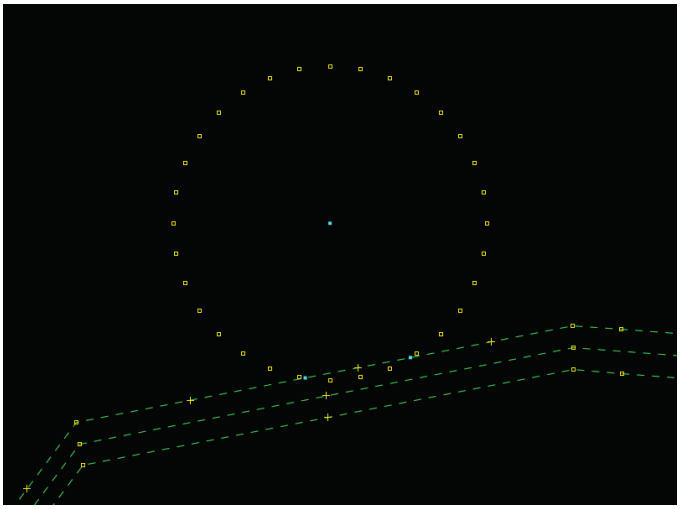

Fig. 1. Sample from our OSRM engine: field of "coverage" (e.g., could be: face detection, face recognition - see Section III-C) of a CCTV camera modelled as 360-degree view intersecting the edge of an OSM way that we then artificially split into two.

directly from the street level imagery. As the annotation tool is a plugin running within the browser, it is also perfectly positioned to parse the browser URLs. Therefore this allows us whenever possible and available to extract the geo-location information from online services such as Google Street View, and then link it precisely to the annotated street-level imagery.

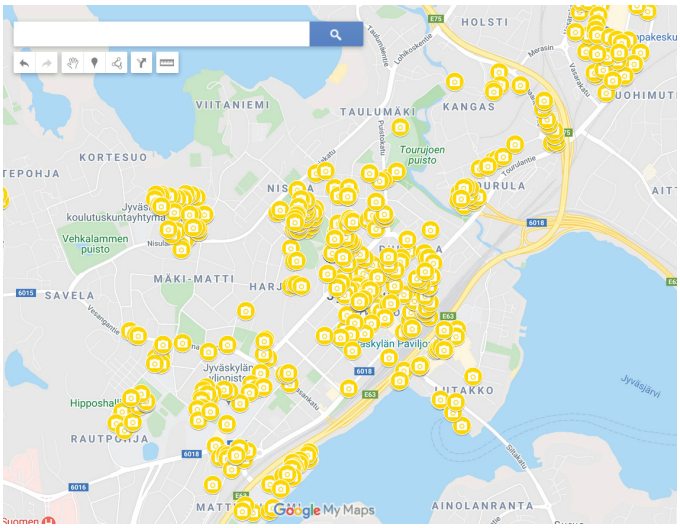

Fig. 2. Data sample depicting a large portion of the entire set of about 450 CCTV cameras that we mapped in Jyväskylä.

C. Coverage of CCTV cameras

Any given CCTV camera has more than a dozen properties that affect its performance and functionality. Even the same camera under different configuration (e.g., resolution, focal length) may have a totally different performance in exactly the same situation (e.g., may be able to recognize a face or not). Moreover, different CCTV cameras have different technical properties and operational settings. When it comes to qualitative tasks, such as license plate identification or

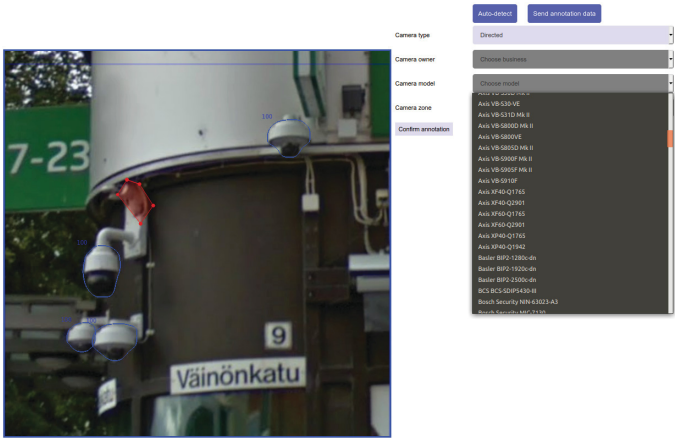

Fig. 3. Screenshot from working with our novel and unique annotation, autodetection and crowdsourcing tool for Computer Vision running as *in-the-browser extension* [23] – in blue are *round* cameras autodetected with pixel-accuracy by the ML models; in red are *directed* cameras manually annotated by the user.

face recognition, there must be a way to compare CCTV cameras regardless of their slightly different capabilities and configurations. Therefore, a metric such as Pixel Per Meter (PPM) (or PPF, see note VI– 1) was introduced which is a measurement used to define the amount of potential image detail that a camera offers at a given distance. Subsequently, various video surveillance tasks (e.g., face recognition) have been assigned a minimum PPM that the camera must support in its operational environment (i.e., resolution, focal length, distance to object) in order to have a chance to successfully perform the said task. According to European Standard EN 62676-4:2015 [13], the following PPM requirements are for various video surveillance tasks:

- Identification – 250 PPM
- Recognition – 125 PPM
- Observation – 62 PPM
- Detection – 25 PPM
- Monitoring – 12 PPM

"Face recognition" means that person can be recognized (but not necessarily identified) from the CCTV footage. *"Automated License Plate Recognition (ALPR)"* means a distance at which cars plate is clearly seen and the car can be identified according to the CCTV footage. For example, for successful ALPR it is required a CCTV vs. object (car) configuration of between 200 PPM (EU license plate) and 400 PPM (Middle East license plate).

Using various experimental setups, the researchers and the manufacturing companies have concluded that with CCTV surveillance grade cameras, on average, the persons can be detected and tracked at distances of 25–50m, and the faces can be recognized at distances of 15–20m [4], [41]. Therefore, when we model the mapped cameras, we assume the following:

- *low-performance cameras* – face recognition successful at a maximum of 10m from the camera
- *medium-performance cameras* – face recognition successful at a maximum of 15m from the camera
- *high-performance cameras* – face recognition successful at a maximum of 25m from the camera

These numbers (i.e., 10m, 15m, 25m) are subsequently driving the types of experiments we plan and test (see Section III-D).

In this preliminary feasibility study, we also chose to employ coarse modelling and apply a set of over-simplifications that apply to a single experimental run, as follows:

- All cameras have a 360-degree Field of View (FoV)
- All cameras up to the extent of "coverage" radius are able to successfully perform "face recognition"
- All cameras have the same properties (same "coverage" radius, resolution, PPM, etc.)

Indeed, under more realistic assumptions, the cameras would have varying "coverage" radius, as well as part of them would be 360-degree view while others would have sectoral FoV. Also, the "coverage" radius to be used for modelling the cameras on the routes would vary according to camera settings (which are unknown to anyone except the camera owner and/or operator) and the surveillance task at hand (e.g., face recognition vs. person detection). Our current model also does not take into account the day vs. night and high-visibility vs. low-visibility (e.g., fog) conditions. Finally, in this paper we study only the feasibility for the walking pedestrian routes. Some future work plans include: evaluations for cycling routes; evaluations for driving routes involving ALPR-related privacy as opposed to face recognition privacy; using (autonomous) cars as mobile devices that emply our CCTV detection models for real-time detection, reporting and mapping of the cameras. We leave all these improvements and refinements as future work.

D. Route points selection

We choose city central area for our routing experiments. We also preferred the most popular walking routes as well as specific places were surveillance cameras can block passage or force routes to use another path. For example, there are railway paths crossing Jyväskylä separating parts of downtown by very few bridges over the railway. Those bridges are well surveyed by CCTV, therefore it is expected that such railway bridge crossings would pose a challenge for privacy-minded users. For example, the results for routing involving the bridges over the railway can be seen in Fig. 4, 5 and 6. The route selection decision was partly helped by the data-intelligence from eÄlytelli Project, which runs a network of IoT sensors scattered across the city of Jyväskylä and provides basic framework for a data-driven SmartCity future. The IoT sensor network can provide insights to possible routes that are most commonly used by pedestrians that carry mobile devices. The final selection of the route points (i.e., departure and arrival) used in our experiments are presented in Table I.

As already mentioned (Section I), our system supports *privacy-first* and *safety-first* routing options. In our experiments we test and evaluate the following routing modes (see Section III-C, Table I):

1) Safety mode with CCTV cameras modelled as 360-degree with 10m radius of "coverage"
2) Privacy mode with CCTV cameras modelled as 360-degree with 10m radius of "coverage"
3) Privacy mode with CCTV cameras modelled as 360-degree with 15m radius of "coverage"

4) Privacy mode with CCTV cameras modelled as 360-degree with 25m radius of "coverage"

While in each of the present experiments we used fixed and same camera parameters (e.g., 360-degree, coverage radius), our system is now ready to support scenarios where each camera is different while having also non-360-degree coverage and a varying "coverage" radius (e.g., according to individual camera's model and settings). This will allow us to model more realistic scenarios as well as allow the users of our system to select what exactly they want safety for or privacy against – face recognition, face identification, ALPR identification, etc. We leave such experiments as future work.

IV. Results

In this section we present the results of the routing experiments described earlier. Table I summarizes our results. The meaning of the headings in the Table I are as follows:

- *Safety [10m]*: The length of the route when all the cameras in OSM/OSRM are configured to have 10m "coverage" and the routing algorithm is configured to produce safety-first routes.
- *Privacy [10m] (overhead)*: The length of the route when all the cameras in OSM/OSRM are configured to have 10m "coverage" and the routing algorithm is configured to produce privacy-first routes. In paranthesis, it also shows the route increse (i.e., overhead) compared to the *Safety [10m]* length for the same departure and arrival points.
- *Privacy [15m] (overhead)*: Similarly as above, but with cameras configured to have 15m "coverage".
- *Privacy [25m] (overhead)*: Similarly as above, but with cameras configured to have 15m "coverage".

From the Table I it is immediately obvious that a person who wants to preserve a higher level of privacy/anonymity is forced to choose a longer route – on average between 1.5x and 5.0x longer, depending on the configurations of the CCTV cameras around the city. While such a result was somehow intuitively expected, our results confirm such hypothesis in a data-driven and evidence-based manner.

As Table I shows, the increase factors for the privacy-preserving routes get higher when the cameras are assumed to be high-performance, i.e., the radius at which they can successfully perform *face recognition* is assumed to be 25m or even 15m. The safety-first routes resulted in an average distance of 860 meters, while privacy-first routes on average were 1.28km or 1.5x longer (camera "coverage" radius 10m), 1.95km or 2.3x longer (camera "coverage" radius 15m), and 4.3km or 5.0x longer (camera "coverage" radius 25m) respectively.

We also hypothesise that for the scenario when "coverage" radius of 25m, the increase factor of 5.0x for the privacy-first mode resulting from our experiments is in fact lower than it should be in reality. One reason for such assumption is that the route engine was not able to draw point-to-point in some cases and we marked some routes when there were more than 100 meters missing from a fully expected route (e.g., Figures 17 and 18). Another reason for such assumption is that route was avoiding cameras so far from the downtown that the route went into areas where cameras are not fully mapped into our database. If our database would contain 100% of existing cameras, the privacy-first route with 25m "coverage" radius would result in even longer routes.

Comparing routing results under different models provides some insights into what are the chances for person to avoiding cameras hence keeping their privacy/anonymity. Our preliminary experiments and results underline the following observations. When modelling low-performance cameras, i.e., their maximum *face recognition* "coverage" radius is 10m, a person has quite decent chances of keeping their privacy/anonymity while navigating common paths and streets, even though the route lengths increases by a factor of 1.5x. However, when modelling the routes under the assumption that the city employs medium- and high-performance cameras (i.e., "coverage" radius is 15m and 25m respectively), it becomes increasingly problematic if not impossible to keep one's privacy/anonymity while moving around especially in the downtown area. For instance, the 15m "coverage" radius model there was one route that is marked as *route not complete*, and the 25m "coverage" radius model there were two (2) *route not complete* and two (2) *no route* results. This also means that keeping the privacy/anonymity and avoiding cameras gets increasingly difficult when the "coverage" radius is increased from 15 to 25 meters.

A. Analysis of some use-cases

In this section we present and analyse a bit deeper some selected use-cases.

One case is presented in the Fig. 4 – 6. It involves a railway crossing scenario, where several over-passage bridges and one under-passage path are the usual routes for pedestrians. The *safety-first* route (Fig. 4) uses one of the two nearest walk/cycle bridges to go over the railway. We confirmed these two bridges feature a set of CCTV cameras on their both ends, therefore it is virtually impossible to enter or exit one of those two bridges without entering a CCTV camera's *face recognition* "coverage". For the same departure and arrival points, the privacy-first route with a 10m "coverage" model (Fig. 5) is 2.5x longer, and with a 15m "covered" model (Fig. 6) it is 4.6x longer. We confirmed that in both privacy-first routes, both alternative bridge (15m model) and under-passage (10m model) are wider than the safety-first bridges hence provide more moving freedom, and do not have CCTV cameras immediately around them or at their entry/exit points. First, it can be observed that even at 15m "coverage" model, this causes pedestrian routing challenges in downtown area and forces a privacy-minded person to perform a huge loop around. Hence, increasing camera's *face recognition* coverage with just 5m, causes a major change for privacy-first routings, which begs the important question – *Which should be the maximum privacy-invasion (e.g., face recognition) distances for CCTV cameras to operate at, so that they perform their safety and crime-deterrent function while preserving balance with privacy/anonymity?* Second, this use-case clearly demonstrates that walk/cycle bridges with strict CCTV camera coverage on its ends are quite challenging for privacy-minded persons. For example, for a person with reduced mobility who also is privacy-minded this is really a problem since they have to give-up on privacy because taking 5.0x longer route may not be an option for them.

TABLE I. SUMMARY OF ROUTING CASES AND EXPERIMENTAL RESULTS FOR THE DOWNTOWN OF JYVÄSKYLÄ, FINLAND.

Route ID	Departure point (GPS)	Arrival point (GPS)	Safety [10m]	Privacy [10m] (overhead)	Privacy [15m] (overhead)	Privacy [25m] (overhead)
1	Vapaudenkatu 34-36 (62.240541, 25.747361)	Satamakatu 3 (62.237443, 25.756073)	760m Figure 10	1.1km (1.4x) Figure 11	1.3km (1.7x) Figure 12	3.9km (5.1x) Figure 13
2	Vapaudenkatu 75 (62.244948, 25.756137)	Sepänkatu 4 (62.242070, 25.752404)	460m Figure 14	480m (1.0x) Figure 15	2.3km (5.0x) Figure 16	no route (N/A) (notes: VI– 4) Figure 17
3	Väinönkatu 13 (62.244868, 25.746953)	Väinönkatu 7 (62.243479, 25.750451)	250m Figure 7	810m (3.2x) Figure 8	880m (3.5x) (notes: VI– 2) Figure 9	no route (N/A) (notes: VI– 4) Figure 18
4	Uno Savolan katu 26 (62.238352, 25.758390)	Hannikaisenkatu 29 (62.240491, 25.751438)	710m Figure 4	1.8km (2.5x) Figure 5	3.3km (4.6x) Figure 6	4.8km (6.8x) Figure 19
5	Hannikaisenkatu 20 (62.244678, 25.746803)	Väinönkatu 13 (62.242510, 25.755215)	800m Figure 20	790m (1.0x) Figure 21	790m (1.0x) Figure 21	1.2km (1.5x) (notes: VI– 2) Figure 22
6	Mattilanniemi 2 (62.232165, 25.736117)	Hannikaisenkatu 20 (62.242510, 25.755215)	2.2km (notes: VI– 3) Figure 23	2.7km (1.2x) (notes: VI– 3) Figure 24	3.1km (1.4x) (notes: VI– 3) Figure 25	7.3km (3.3x) (notes: VI– 2,3) Figure 26
–	–	Average	860m	1.28km (1.5x)	1.95km (2.3x)	4.3km (5.0x) (notes: VI– 5)

Another case is presented in the Fig. 7 – 9, and it covers a walking street in the center of Jyväskylä (*"Väinönkatu"*). In this case, the arrival point is located in one of the most camera-dense areas. The safety-first route (Fig. 7) takes straight line from departure to arrival points, both of which are located on V¨ain¨onkatu. While safety-first route goes straight, the privacy-first routes with both 10m and 15m "coverage" models are forcing a loop around Kalevankatu. The main difference between the 10m model (Fig. 8) and the 15m model (Fig. 9) is that the 15m model route does not reach the arrival point – the route ends in the backyard of the commercial buildings which is the nearest point where routing can get while avoiding the en-route cameras.

As yet another case, the Fig. 9, 22 and 26 present situations where the route cannoe be successfully completed from point-to-point assuming the users wants to preserve their privacy. Fig. 26 presents an almost complete route, just missing about 10 meter from the "middle point". Fig. 22 shows that the route is missing departure point by about 10 meters. And in Fig. 9, the final part of the V¨ain¨onkatu is blocked by the cameras and the route ends up in the backyard on the wrong side of the building.

It is also important to note the following final observations. Firstly, if the route cannot be calculated "close enough" to the departure or arrival point, the route is not output and not drawn. Secondly, the CCTV camera density is so high in the downtown area that it is not possible to compute privacy-preserving routes in some cases when "coverage" radius is over 20 meters, thus resulting in *no route* situations. Thirdly, in some rare cases the *safety-first* route can be longer than the *privacy-first* one. For example, this can occur if both models (i.e., safety, privacy) are routed over the same rounded curve, and the cameras' "coverage" forces the privacy route towards the inner (shorter) curve while forcing the safety route towards the outer (longer) curve.

The rest of the visual results that correspond to our experiments can be found in Section VI-A.

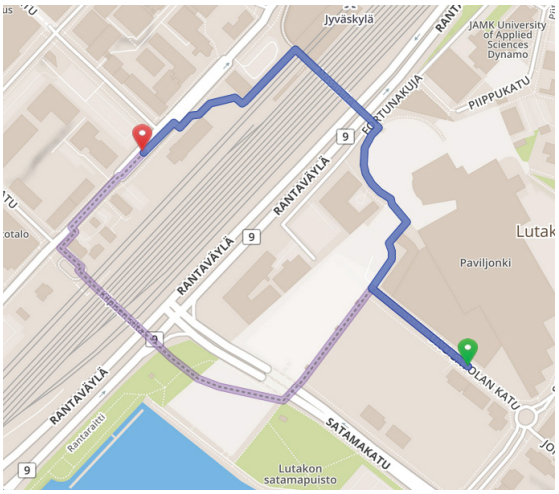

Fig. 4. Route ID 4 – safety-first with 10m radius model, distance 710m

V. CONCLUSION

In this paper we studied the feasibility of developing CCTV-aware technology for privacy-first and safety-first routing and navigation, as well as the impact and difference between privacy-first and safety-first approaches. For this, we created initial working prototypes of routing engine based on open-source OSRM framework. To support our initial exploration, we developed and experimented with somewhat simplified models involving CCTV cameras' mapping, cameras' coverage and corresponding privacy/safety impact. In addition, we relied in our efforts on some of our previous

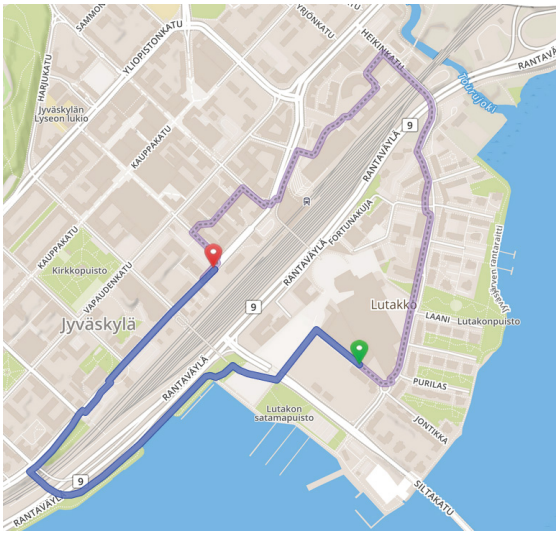

Fig. 5. Route ID 4 – privacy-first with 10m radius model, distance 1.8km

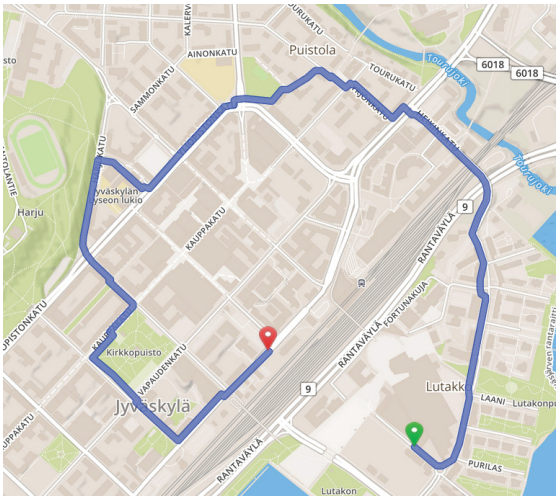

Fig. 6. Route ID 4 – privacy-first with 15m radius model, distance 3.3km

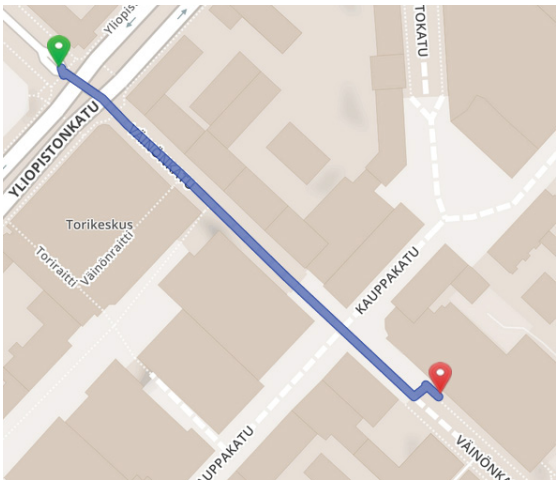

Fig. 7. Route ID 3 – safety-first with 10m radius model, distance 250m

works and ideas such as accurate and instant detection and

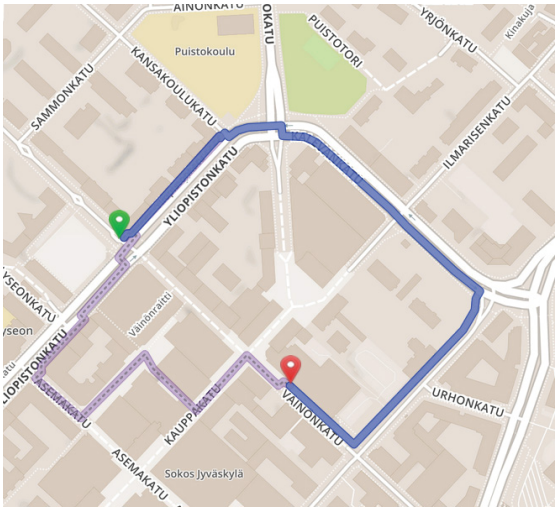

Fig. 8. Route ID 3 – privacy-first with 10m radius model, distance 810m

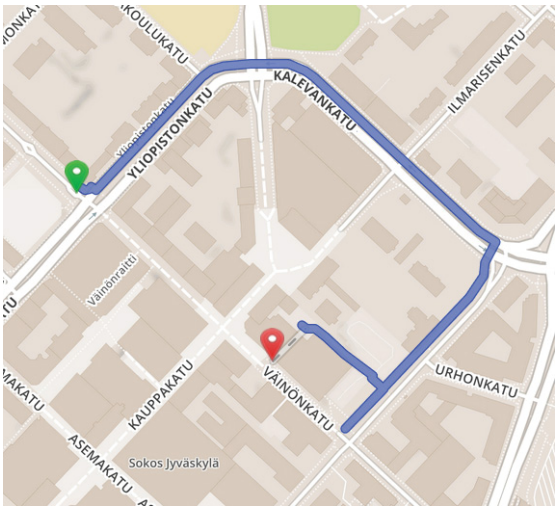

Fig. 9. Route ID 3 – privacy-first with 15m radius model, distance 880m. (notes: VI– 2)

mapping of CCTV cameras using automated Computer Vision and manual crowdsourcing and annotation approaches.

To prove our CCTV-aware approach is feasible, we run our experiments on real-world data-driven scenarios for downtown of the city of Jyväskylä, Finland. Our results are encouraging (for further research) and worrying (for privacy-minded persons) at the same time. Firstly, our experiments and results clearly demonstrate that our CCTV-aware technology works and can potentially bring lots of added-value to researchers, citizens, and policy-/decision-makers. This encourages us to improve and refine our models and implementations, and run much larger scale experiments based on richer and more accurate CCTV cameras datasets. Therefore we invite interested parties (e.g., city administrations, governments) to contact us for joint-research towards SmartCities that are safe thanks to CCTV yet provide equal and privacy-preserving opportunities to all. Secondly, our experiments clearly show that there is an obvious and quantifiable impact for privacy-minded persons. The overall impact is negative both on quantitative dimension (e.g., distance increase), and qualitative dimension (e.g.,

some routes are impossible with full privacy/anonymity). For example, based on the data and models we used, the privacy-minded users suffer on average a distance increase between 1.5x to 5.0x (depending on the model applied) when compared to no-preference or safety-oriented users. While increasing and improving the datasets and the models will certainly result in different impact results, we expect the change to be even more towards a negative side for the privacy-minded users. One reason for such an expectation is the fact that our current CCTV camera dataset is just a subset of all the CCTV cameras deployed in the real-world, i.e., the count of cameras we use in our modelling and route estimation is (considerably) smaller than in reality.

Finally, we argue that in order to move the discussion beyond subjective and futile debates such as "CCTVs are good vs. CCTVs are bad", technology must be efficiently used and data-driven decision and analysis must be applied. This in turn prompts that the governments and administrations release and maintain as open-data detailed registries of both publicly- and privately-operated CCTV cameras. Such open-data will allow the users and decision makers to use CCTV-aware technology such as ours, therefore can make better decisions (e.g., routing for users, policies for decision-makers).

VI. Notes and Remarks

1) For non-metric jurisdictions, Pixel Per Foot (PPF) is als defined and often used.
2) The *route not complete* result is when some final distance cannot be included in the route (cameras would break the privacy-preserving requirement).
3) The routes were intentionally instructed to have an intermediate stop-point at Kauppakatu 18 (62.241531, 25.745317).
4) The engine was unable to generate a privacy-preserving route close to arrival point (when using given cameras modelling and given OSM data).
5) The *no route* results are ignored from the calculation of average data.

Acknowledgments

We acknowledge grants of computer capacity from the Finnish Grid and Cloud Infrastructure (FGCI) (persistent identifier `urn:nbn:fi:research-infras-2016072533`).

Part of this research was kindly supported by the *"17.06.2020 Decision of the Research Dean on research funding within the faculty"* grant from the Faculty of Information Technology of the University of Jyväskylä, and the grant was facilitated and managed by Dr. Andrei Costin.

We also thank Prof. Timo Hämäläinen and Riku Immonen for providing data-intelligence from eÄlytelli Project [1] – Ecological, intelligent and secured IoT services – a project funded by the European Regional Development Fund (ERDF) and the partner companies involved.

References

[1] "eÄlytelli Project – Ecological, intelligent and secured IoT services – a project funded by the European Regional Development Fund (ERDF)," https://ealytelli.fi/in-english/.

[2] "Google Street View," https://www.google.com/streetview/explore/.

[3] "How Many CCTV Cameras in London?" https://www.caughtoncamera.net/news/how-many-cctv-cameras-in-london/.

[4] Axis, "Identification and recognition," https://www.axis.com/files/feature_articles/ar_id_and_recognition_53836_en_1309_lo.pdf.

[5] S. Bao, T. Nitta, K. Ishikawa, M. Yanagisawa, and N. Togawa, "A safe and comprehensive route finding method for pedestrian based on lighting and landmark," in *2016 IEEE 5th Global Conference on Consumer Electronics*, 2016, pp. 1–5.

[6] H. Bast, D. Delling, A. Goldberg, M. Müller-Hannemann, T. Pajor, P. Sanders, D. Wagner, and R. F. Werneck, "Route planning in transportation networks," in *Algorithm engineering*. Springer, 2016.

[7] BBBike.org, https://www.bbbike.org/, 2020.

[8] bikecitizens.net, "Discover and share the joy of cycling," https://www.bikecitizens.net/.

[9] E. Cosgrove, "One billion surveillance cameras will be watching around the world in 2021," https://cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html.

[10] K. Deilami, J. Rudner, A. Butt, T. MacLeod, G. Williams, H. Romeijn, and M. Amati, "Allowing Users to Benefit from Tree Shading: Using a Smartphone App to Allow Adaptive Route Planning during Extreme Heat," *Forests*, vol. 11, no. 9, p. 998, 2020.

[11] D. Delling, P. Sanders, D. Schultes, and D. Wagner, "Engineering route planning algorithms," in *Algorithmics of large and complex networks*. Springer, 2009.

[12] G. developers, https://geopandas.org/. [Online]. Available: https://github.com/geopandas/geopandas

[13] B. EN, "62676-4: 2015. Video surveillance systems for use in security applications," *British Standard Institution*, pp. 1–82, 2015.

[14] A. Franco, "What is curvature?" 2016, [Online; accessed 1-November-2020]. [Online]. Available: https://roadcurvature.com/

[15] S. Gillies, "The shapely user manual," https://shapely.readthedocs.io/en/stable/manual.html, 2020.

[16] H. I. f. G. T. H. GIScience, https://openrouteservice.org/, 2020.

[17] S. Hoffmann, "Osmium library," https://osmcode.org/pyosmium/.

[18] W. Hu, T. Tan, L. Wang, and S. Maybank, "A survey on visual surveillance of object motion and behaviors," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 34, no. 3, pp. 334–352, 2004.

[19] B. Karas, "Americans Vastly Underestimate Being Recorded on CCTV," https://ipvm.com/reports/america-cctv-recording.

[20] P. Kasemsuppakorn and H. A. Karimi, "Personalised routing for wheelchair navigation," *Journal of Location Based Services*, vol. 3, no. 1, pp. 24–54, 2009. [Online]. Available: https://doi.org/10.1080/17489720902837936

[21] A. Keler and J. D. Mazimpaka, "Safety-aware routing for motorised tourists based on open data and vgi," *Journal of location Based services*, vol. 10, no. 1, pp. 64–77, 2016.

[22] komoot.com, "What is komoot?" https://www.komoot.com/about.

[23] T. Lahtinen, H. Turtiainen, and A. Costin, "BRIMA: Low-overhead Browser-Only Image Annotation Tool (Preprint)," *arXiv preprint*, 2021.

[24] M. Lucas-Smith, "Is the osm data model creaking?" https://2019.stateofthemap.org/sessions/DW7WW8/.

[25] D. Luxen, "[OSM-dev] Announcing the immediate availability of the Open Source Routing Machine," https://lists.openstreetmap.org/pipermail/dev/2010-July/019834.html, 2010.

[26] D. Luxen and C. Vetter, "Real-time routing with OpenStreetMap data," in *Proceedings of the 19th ACM SIGSPATIAL international conference on advances in geographic information systems*, 2011.

[27] ——, "Real-time routing with OpenStreetMap data," in *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, ser. GIS '11. New York, NY, USA: ACM, 2011, pp. 513–516. [Online]. Available: http://doi.acm.org/10.1145/2093973.2094062

[28] K. Ma, "Parasol: Shade model and routing algorithm for comfortable travel outdoors," https://github.com/keithfma/parasol.

[29] ——, "Parasol Navigation: Optimizing walking routes to keep you in the sun or shade," https://www.allnans.com/jekyll/update/2018/08/07/introducing-parasol.html, 2018.

[30] H. Miura, S. Takeshima, N. Matsuda, and H. Taki, "A study on navigation system for pedestrians based on street illuminations," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. Springer, 2011, pp. 49–55.

[31] T. Novack, Z. Wang, and A. Zipf, "A system for generating customized pleasant pedestrian routes based on openstreetmap data," *Sensors*, vol. 18, no. 11, p. 3794, 2018.

[32] C. Olaverri Monreal, M. Pichler, G. Krizek, and S. Naumann, "Shadow as Route Quality Parameter in a Pedestrian-Tailored Mobile Application," *IEEE Intelligent Transportation Systems Magazine*, vol. 8, no. 4, pp. 15–27, 2016.

[33] OpenStreetMap, "Routing/offline routers," https://wiki.openstreetmap.org/wiki/Routing/offline_routers.

[34] ——, "Routing/online routers," https://wiki.openstreetmap.org/wiki/Routing/online_routers.

[35] Project-OSRM, "Traffic," https://github.com/Project-OSRM/osrm-backend/wiki/Building-with-Mason, 2019.

[36] ——, "Osrm profiles," https://github.com/Project-OSRM/osrm-backend/blob/master/docs/profiles.md, 2020.

[37] I. Scholz, D. Stcker, and other contributors, https://josm.openstreetmap.de/, 2020.

[38] R. J. Szczerba, P. Galkowski, I. S. Glicktein, and N. Ternullo, "Robust algorithm for real-time route planning," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 36, no. 3, pp. 869–878, 2000.

[39] J. Topf, "Osmium library," https://osmcode.org/libosmium/.

[40] H. Turtiainen, A. Costin, T. Lahtinen, L. Sintonen, and T. Hamalainen, "Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision. Applications and implications for privacy, safety, and cybersecurity.(Preprint)," *arXiv preprint arXiv:2006.03870*, 2020.

[41] F. W. Wheeler, R. L. Weiss, and P. H. Tu, "Face recognition at a distance system for surveillance applications," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 2010, pp. 1–8.

[42] O. Wiki, "Editors — openstreetmap wiki," 2020, [Online; accessed 2-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=Editors\&oldid=2053356

[43] ——, "Josm — openstreetmap wiki,," 2020, [Online; accessed 8-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=JOSM\&oldid=2034195

[44] ——, "List of osm-based services — openstreetmap wiki," 2020, [Online; accessed 1-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=List_of_OSM-based_services\&oldid=2052956

[45] ——, "Osm xml — openstreetmap wiki," 2020, [Online; accessed 5-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=OSM_XML\&oldid=2027286

[46] ——, "Osmosis — openstreetmap wiki," 2020, [Online; accessed 2-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=Osmosis\&oldid=2035526

[47] ——, "Way — openstreetmap wiki," 2020, [Online; accessed 2-November-2020]. [Online]. Available: https://wiki.openstreetmap.org/w/index.php?title=Way\&oldid=2045405

[48] A. Zipf, A. Mobasheri, A. Rousell, and S. Hahmann, "Crowdsourcing for individual needsthe case of routing and navigation for mobility-impaired persons," *European Handbook of Crowdsourced Geographic Information*, pp. 325–337, 2016.

APPENDIX

A. All routing samples

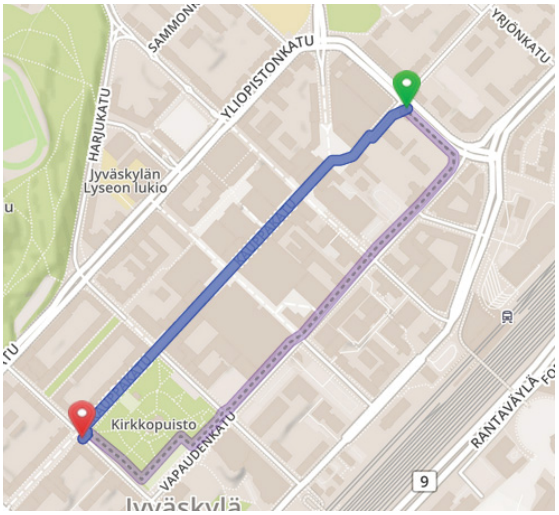

Fig. 10. Route ID 1 – safety-first with 10m radius model, distance 760m

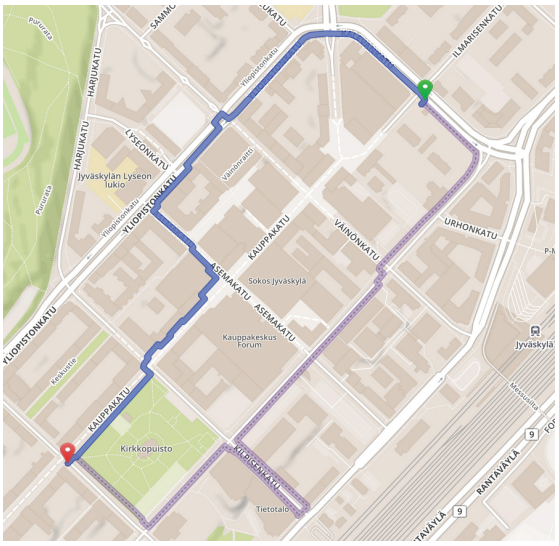

Fig. 11. Route ID 1 – privacy-first with 10m radius model, distance 1.1km

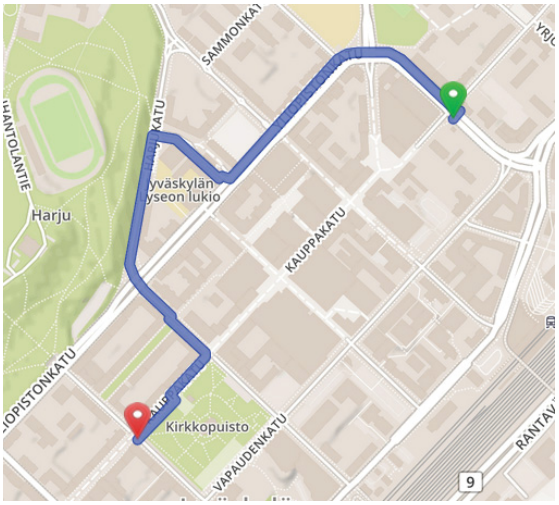

Fig. 12. Route ID 1 – privacy-first with 15m radius model, distance 1.3km

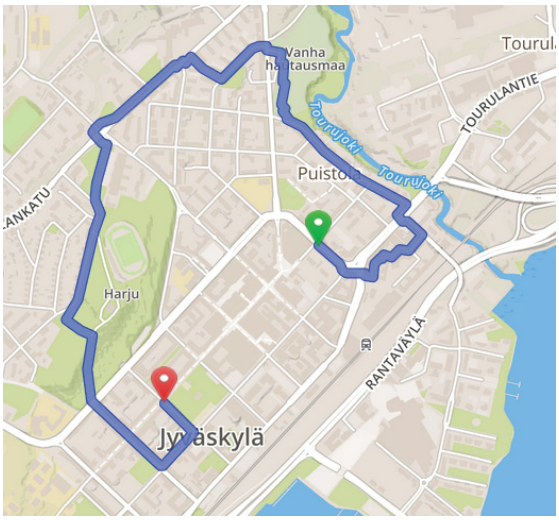

Fig. 13. Route ID 1 – privacy-first with 25m radius model, distance 3.9km. (notes: VI– 4)

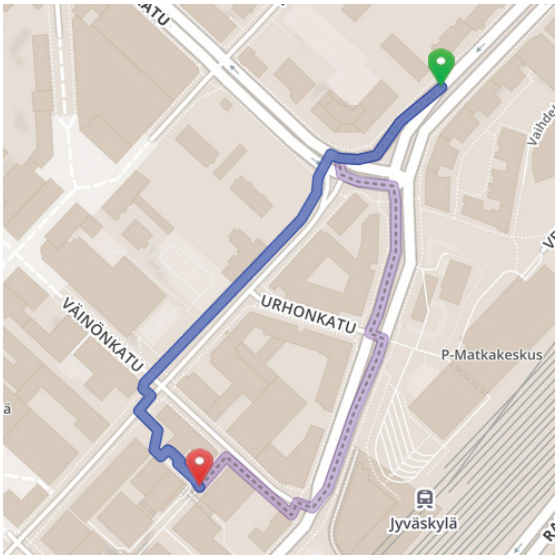

Fig. 15. Route ID 2 – privacy-first with 10m radius model, distance 480m

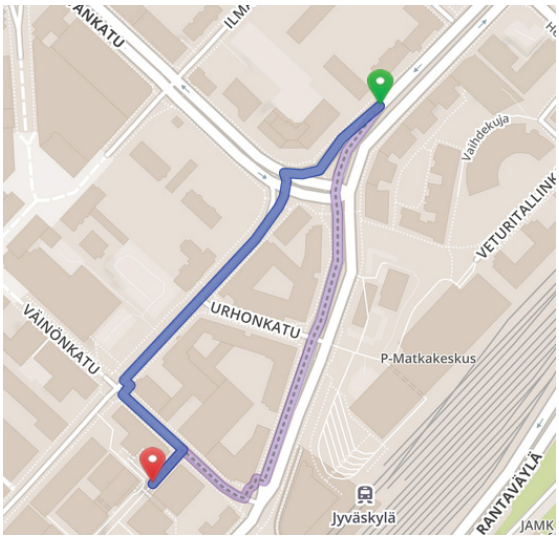

Fig. 14. Route ID 2 – safety-first with 10m radius model, distance 460m

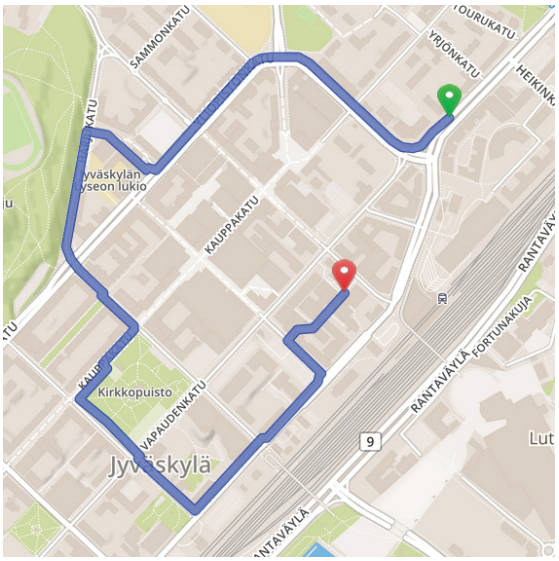

Fig. 16. Route ID 2 – privacy-first with 15m radius model, distance 2.3km

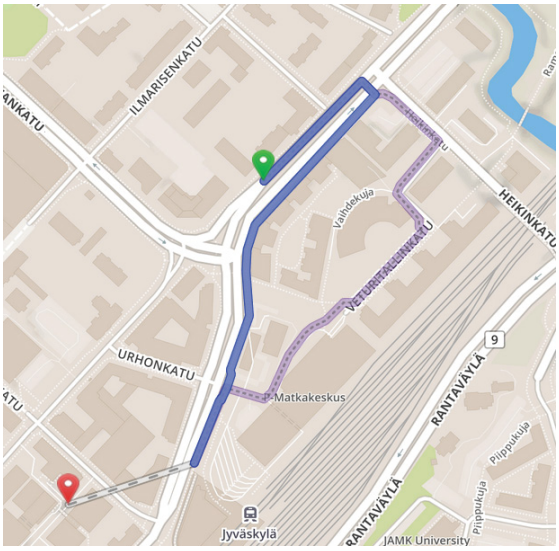

Fig. 17. Route ID 2 – privacy-first with 25m radius model – no route. (notes: VI– 4)

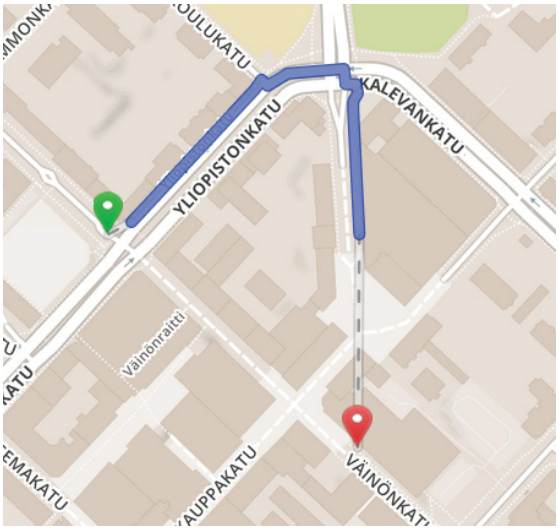

Fig. 18. Route ID 3 – privacy-first with 25m radius model – no route. (notes: VI– 4)

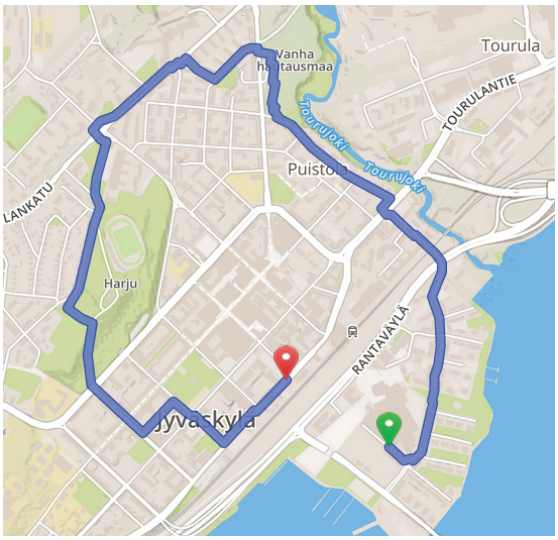

Fig. 19. Route ID 4 – privacy-first with 25m radius model – distance 4.8km

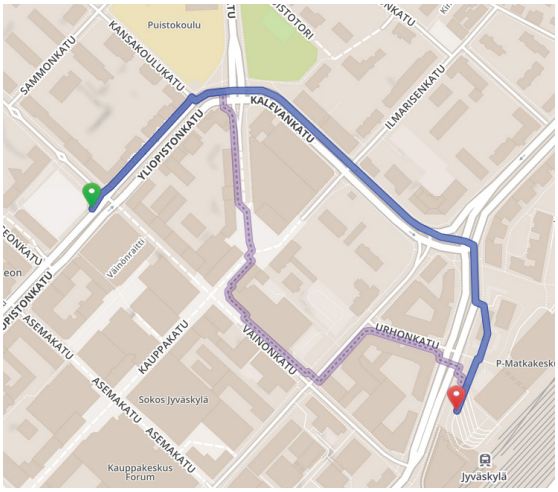

Fig. 20. Route ID 5 – safety-first with 10m radius model, distance 800m

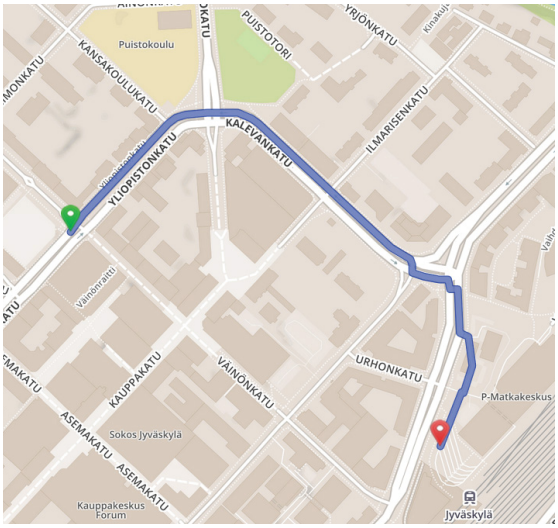

Fig. 21. Route ID 5 – privacy-first with 10 and 15m radius model, distance 790m

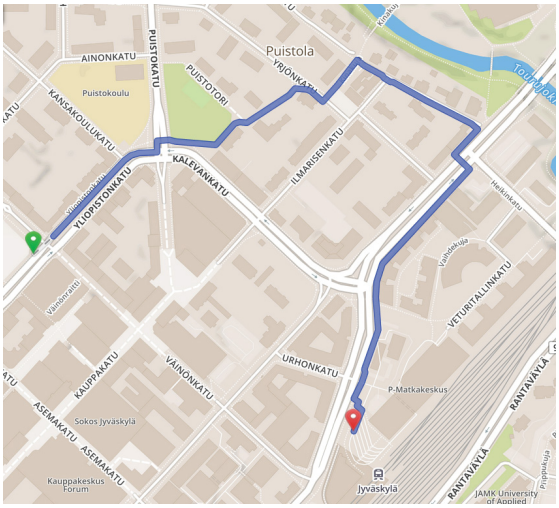

Fig. 22. Route ID 5 – privacy-first with 25m radius model, distance 1.2km. (notes: VI– 2)

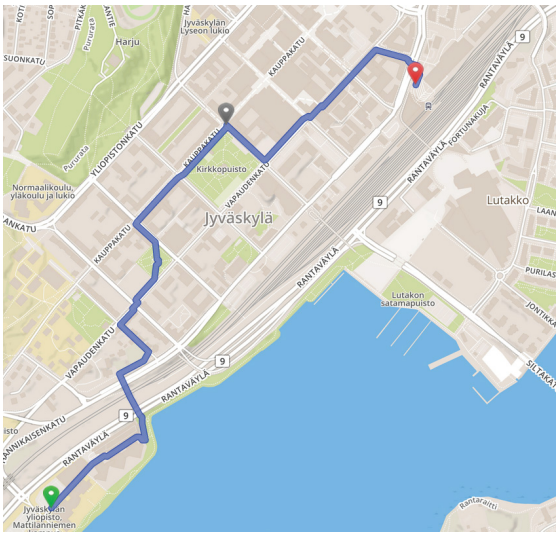

Fig. 23. Route ID 6 – safety-first with 10m radius model, distance 2.2km. (notes: VI– 3)

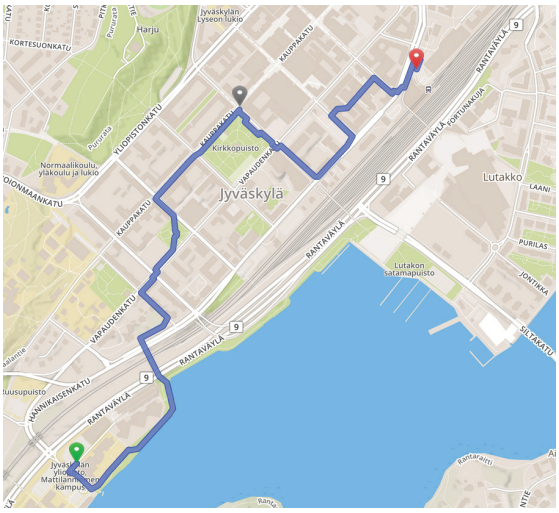

Fig. 24. Route ID 6 – privacy-first with 10m radius model, distance 2.7km. (notes: VI– 3)

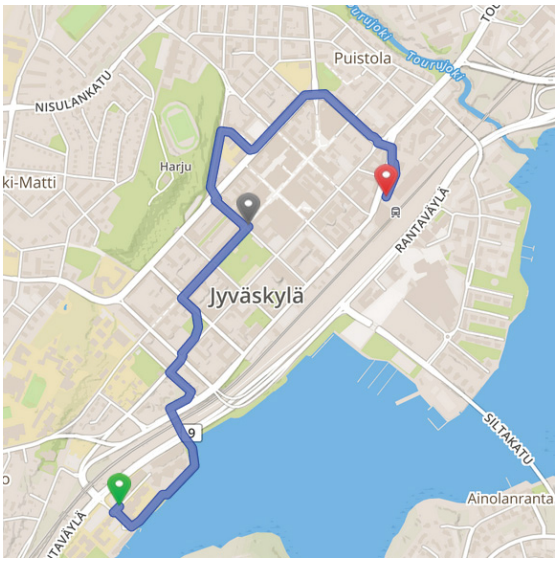

Fig. 25. Route ID 6 – privacy-first with 15m radius model, distance 3.1km. (notes: VI– 3)

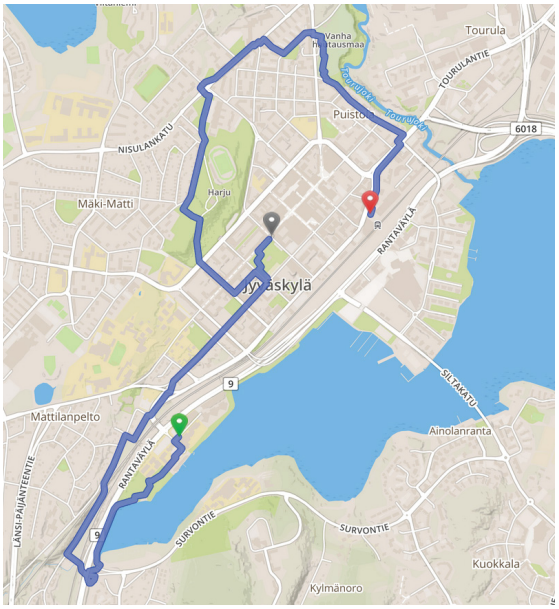

Fig. 26. Route ID 6 – privacy-first with 25m radius model, distance 7.3km. (notes: VI– 2,3)